E-Safety Policy

1. Introduction

The rapid developments in electronic communications are having many effects on society. The Internet is a part of everyday life for education, business and social interaction. The School has a duty to provide pupils with quality Internet access as part of their learning experience. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. At the School we use electronic communications in a number of ways and this policy outlines our commitment to e-safety and the steps we will take to ensure our children are safe.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- access to experts in many fields for staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates by Wolverhampton City Council;
- exchange of curriculum and administration data with Wolverhampton City Council and DfE;

2. Roles and Responsibilities

The school recognises that as a small setting it is challenging to have sufficient separation of responsibility for e-safety and therefore an annual service level agreement is purchased from the Local Authority to provide technical support and to manage the schools IT systems.
The roles and responsibilities for e-safety are:

Head Teacher

- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and procedures
- Liaises with the Local Authority and IT Technical staff on matters relating to e-safety
- Ensures that staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Has responsibility for ensuring appropriate procedures are followed in the event of a serious e-safety allegation being made against a member of staff.
- Is responsible for ensuring that staff receive appropriate training to enable them to carry out their role safely.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety

Technical Staff (Local Authority)

- Ensure the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensure that users may only access the networks and devices through a properly enforced password protection policy
- Ensure that the network, internet, remote access and email systems can be regularly monitored in order that misuse/attempted misuse can be identified.

Staff

- Ensuring they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- Ensure they have read and understood the Acceptable Use Policy
- Must report any suspected misuse or problem to the Head Teacher.
- Ensure all digital communications with parents are on a professional level and are only carried out using official school systems
- In lessons where internet use is pre-planned ensure that sites have been checked as suitable for use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Ensure the school's technical infrastructure is secure and is not open to misuse or malicious attack

3. Using the Internet to Enhance Teaching and Learning

- The School's Internet access will be designed to enhance and extend education.
- Children will only be given access to the internet under the direct supervision of a member of staff.
- Staff must check the content of a web-site thoroughly before use with children and must seek permission from senior staff before allowing children to access a new web-site.
- The School will ensure that the copying and subsequent use of Internet derived materials by staff complies with copyright law.
- Staff will guide children to online activities that will support learning outcomes and that are appropriate for their age.
- Staff will acknowledge the source of information used and respect copyright when using Internet material in their own work.

4. Managing Information Systems

The School has a Local Area Network (LAN). In managing the system the following applies:

- Staff are responsible for their personal network area.
- Line Managers are responsible for overseeing their team network area and removing unwanted files.
- Servers are located securely and physical access is restricted.

- The server operating system is secured and kept up to date. This is managed by the local authority ICT Dept through an annual service level agreement.
- Virus protection for the whole network is installed and maintained by the local authority ICT Dept.

Wide Area Network (WAN) security issues include:

- All Internet connections are arranged by the local authority ICT team to ensure compliance with the security policy.

Additional security measures taken:

- Personal data may only be sent by email using the school's secure email of which only the Head Teacher has access.
- Sensitive information will only be sent following the Council's secure email policy and emails will be labelled according to the level of sensitivity of the information.
- Portable media such as memory sticks or portable drives may **NOT** be used without specific permission of the Head Teacher followed by a virus check.
- Unapproved software is not permitted
- Files held on the school's network will be regularly checked.
- The ICT support team will review system capacity regularly.

5. Managing Email

Email is an essential means of communication for staff.

- Emails made by a member of staff with a group of pupils must be made using a group or project email.
- Personal details of staff or children must not be revealed in emails.
- Social email use is restricted.
- Access in work to external personal email accounts is not permitted and may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes

6. Published Materials – Web-sites

The School has commissioned the development of a web-site which is managed by the local authority ICT team. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

7. Social Media

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their

employment. Access to social network sites is not permitted and are filtered and blocked by the Local Authority. Staff are required to follow the guidance within the staff handbook and code of conduct regarding the use of social networking outside of school. Social networking will not be undertaken with pupils due to their age and stage of development.

The following measures are designed to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information via social media.

- No reference should be made to the school, pupils, staff or parents
- Staff must not engage in online discussion relating to members of the school community
- Personal opinions should not be attributed to the school
- Staff must not disclose their role or place of work
- Security settings on staff personal social media profiles should be regularly checked to minimise the risk of loss of personal information

8. Managing Personal Data

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 (“the Act”) gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual’s rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

9. Internet access

- The school will allocate Internet access for staff on the basis of educational need and according to their role.

- The school will maintain a current record of all staff who are granted access to the school's electronic communications.
- All staff must read and sign the Acceptable Use Policy before using any school ICT resource.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

10. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff instant use of images they have recorded themselves or downloaded from the internet. However, staff must be aware of the risks associated with the publication and use of digital images.

- When using digital images, staff must ensure that they have appropriate permissions from parents/carers for the use of the image
- Images taken of children to evidence learning can only be downloaded and stored securely on the schools internal server.
- Staff should ensure that when taking digital images/videos that pupils are appropriately dressed
- Images can only be taken on school equipment.
- Images of pupils must remain on school site and must not be sent via email or other electronic communications.
- Photographs published on the school website or in other publications will be selected carefully and will not be used without the express permission of the child's legal guardian.

11. Reporting Incidents of Misuse

Where an incident occurs or there is suspicion that there may be a breach of the e-safety policy staff should report their concerns to the Head Teacher or Senior Manager in her absence. Any policy breach will be investigated and a written record kept. Where an allegation is made against another member of staff the school will consult with its HR Consultant and follow the disciplinary policy where this is appropriate.

Illegal Use

If there is any suspicion that a web-site which has not been blocked by the school's filtering system is suspected of containing illegal activity or material, this must be reported to the Head Teacher and reported to the police.

It is hoped that all members of the school community will be responsible users of digital technologies, however there may be times when infringements of the policy could take place, through careless or irresponsible, or very rarely, through deliberate misuse.

In the event of suspicion:

- The Head Teacher or Senior Members of staff in her absence, must be informed as soon as a suspicion is raised
- Advice and guidance regarding appropriate disciplinary actions will be taken from the School's HR Consultant
- An investigation will be undertaken by a Senior Member of staff with the support of the IT Technician to gain evidence including URL addresses and log in information.
- Where appropriate screen shots may be taken
- If content being reviewed includes images of Child abuse the Police will be contacted immediately.
- If appropriate hardware will be isolated whilst an investigation takes place.

Inappropriate Use

It is more likely that incidents of misuse involve inappropriate rather than illegal actions. As with more serious incidents any breach of policy should be reported to a senior member of staff who will investigate this matter. If a disciplinary investigation is required the Schools disciplinary procuress will be followed.

This list is not exhaustive but should be used as guidance as to the types of activities that are deemed inappropriate.

- Deliberately accessing or trying to access material that could be considered to be illegal
- Inappropriate personal use of the internet / social media / personal email
- Unauthorized downloading or uploading of files
- Allowing others to access the school network by sharing username and passwords
- Careless use of personal data including transferring data in an unsecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal email / social networking / instant messaging / text messaging to carry out digital communication with pupils or their parents
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the schools filtering system
- Accidentally accessing or trying to access offensive material
- Breaching copyright or licensing regulations

Approved at a Full Governing Body Meeting on 2nd February 2016